Security praktisch

S E C U R I T Y - P R A K T I S C H

> ***Das Produkt aus Security und Bequemlichkeit ...***
> ***...ist endlich und indirekt proportional!***

Physikalischer Zugang zur Direktion

Wer hat Zugang zur Direktion und damit Zugang zum Rechner samt Datensicherung (ext. Platte, USB-Stick, …)?

- Zutrittsschutz
- Datensicherung auf externen Datenträgern getrennt aufbewahren (z. B. im Safe)

Inbetriebnahme des Rechners - Kennwort

Kann Ihr Rechner ohne Kennwort in Betrieb genommen werden?

- Bios-Schutz mittels Kennwort
- Pre-Boot-Authentification beim Start des Rechners
- Kennwortschutz beim Start des Betriebssystems
- Kennwörter (niemals aufgeklebt am Tisch, am Monitor, …)
- Start mit externen Datenträgern

Tipp 1:

Wenn Kennwörter schon aufgeschrieben werden, bitte jedenfalls sicher/im Safe verwahren!

Kennwortsicherheit

Die sorgfältige Verwendung und Geheimhaltung von Zugangsdaten (Benutzerkennung und Passwort) ist der am häufigsten angesprochene Punkt im Hinblick auf die Thematik "Security". Seitens des Ministeriums wird vor einer elektronischen Speicherung von Zugangsdaten unabhängig vom Speicherort abgeraten.

Wie sicher ist Ihr Kennwort zum Start vom Betriebssystem (Windows) und wie sicher sind Ihre Kennwörter für kritische Anwendungen (Mail, Portal, ...)?

- Komplexität, Änderungszyklus, Sperrung nach Fehlversuchen, Admin-Konto mit Überwachung (Anmeldeversuche werden mitgeloggt – Missbrauch fliegt auf!), …
- Verwendung von Passwort-Managern (keepass o. ä.) - achten Sie dabei auf 2-Wege-Sicherheit (Datei und Masterpasswort in Kombination bilden den Schüssel zur Passwortsammlung) und nehmen Sie Zugangskennungen für sensible Daten lt. DSG nicht darin auf, wie vom Ministerium empfohlen
- Gespeicherte Kennwörter im Browser vermeiden
- Unterscheide:
  Persönliches TSN-Kennwort (Portalanwendungen)
  Direktionsmail-Kennwort (Funktionspostfach)
- Berufliche Kennwörter niemals auch im privaten Bereich (in sozialen Netzwerken etc.) verwenden

- Mailclientstart mit Passwort-Abfrage
- Welche Benutzerkonten mit welchen Berechtigungen sind auf dem Rechner eingerichtet?
- Ist das Datenverzeichnis (z. B. D:\Daten-Schule) für alle angemeldeten Benutzer lesbar?
- Arbeiten als PC-User (Hauptbenutzer),
  PC-Administrator nur für höhere Rechte bei Installationen etc. verwenden
  (UAC – Benutzerkontensteuerung einschalten),
  nicht idente Kennwörter bei verschiedenen Anwendungen verwenden

Tipp 2:

Nicht "1PW4all" (one password for all);
verschiedene Anwendungen, verschiedene Kennwörter!

Anleitung zum Ändern des TSN-Kennworts --> hier!

Datensicherheit

Wie sicher sind Ihre Daten am Rechner oder im Netzwerk? Wie verantwortungsbewusst gehen Sie mit wichtigen Unterlagen um?

- Wichtige Unterlagen liegen niemals ungeschützt oder offen herum (Schreibtisch, USB-Stick o. Ä.)
- Dokumente mit personenbezogenen Informationen niemals ohne zusätzlichen Schutz über das offene Internet versenden
- Lokales Profil oder Serverprofil
- Freigegebene Ordner lokal
- Freigaben am Server bezüglich Direktion
  Zugriffssicherheit am Server für Direktionsdaten oder zusätzliche -sicherungen
- WLAN-Verbindung mit Dir-Gerät und Sicherheit
  (eingeschränkt empfohlen)

Tipp 3:

Ihre IT-Betreuung o. ä. Supporteinrichtungen werden niemals die Übermittlung Ihrer Zugangsdaten (Passwort, Pincode, ...) verlangen!

Geundsheitsblätter - Bsp. für sensible Daten

Wie verhält es sich mit den Gesundheitsblättern an der Schule (Führung, Einsicht, Auskunft, Weitergabe, ...)?

- Amtsschriftenverordnung vom LSR regelte seinerzeit die Aufbewahrungsfristen (Gesundheitsblätter - 3 Jahre nach Ende des Schuljahres/Austritt)
- verschlossene Lagerung im Schularztzimmer bzw. in der Direktion und nur für den Schularzt zugänglich
- Elternfragebögen oder Mitteilungen der Eltern an die Schulärztin/den Schularzt in verschlossenen Kuverts dürfen nur von der betroffenen Schulärztin/vom betroffenen Schularzt geöffnet werden!
- Weitergabe an Eltern nach Ablauf der Aufbewahrungsfrist bedenkenlos
- Weitergabe an andere Schulen - § 1 Abs 1 und 2 DSG (Datenschutzgesetz; Grundrecht auf Datenschutz)
- Nach Ablauf der Aufbewahrungsfrist sind jene Gesundheitsblätter zu vernichten, die nicht an die Schüler ausgehändigt wurden

- Liegt eine Zustimmung zur Weitergabe vor, wird vom Grundrecht auf Datenschutz nicht Gebrauch gemacht und einer Weitergabe der Daten an die aufnehmende Schule steht rechtlich nichts entgegen
- Bei digitaler Erfassung der Gesundheitsdaten werden auch andere Bestimmungen schlagend!
- Auskunft: aufscheinende medizinische Daten müssen dem Schüler/der Schülerin bzw. seinen Erziehungsberechtigten jederzeit auf Anfrage bekannt gegeben werden (§ 66 Abs 2 SchUG sowie DSG 2000), unabhängig davon, ob gesundheitliche Mängel festgestellt wurden. Eine direkte Einsichtnahme in das Gesundheitsblatt kann wohl nicht verweigert werden.
- Vom Schularzt waren lt. Amtsschriftenverordnung seinerzeit folgende Aufzeichnungen zu führen: Gesundheitsblätter, Elternfragebögen, Mitteilungen des Schularztes an die Eltern, Aufzeichnungen im Rahmen der schulärztlichen Untersuchung

Verwendung von vorgesehenen Formularen - verfügbare Drucksorten:
http://www.bmg.gv.at/home/Schwerpunkte/Praevention/Schulgesundheit/Schulaerztliche_Drucksorten_Elternfragebogen_und_Gesundheitsblatt

1-jährig und 3-jährig:
http://www.schule.at/dl/Gesundheitsblatt_2007_%28dreijjaehrig%29.pdf
http://www.schule.at/dl/Gesundheitsblatt_Stand_17_2_09.pdf

Erlass Schulgesundheitsstatistik: http://www.eduhi.at/dl/40000-39-2001.pdf

Weitergabe von Schülerdaten - Artikel in der Tageszeitung Der Standard: http://derstandard.at/1265851951200/Weitergabe-von-Schuelerdaten-nicht-zulaessig

Detaillierterer Artikel zu dieser Thematik --> hier!

Datensicherung

Haben Sie eine aktuelle und eine funktionierende Datensicherung? Testen Sie von Zeit zu Zeit Ihre Datensicherung - wird wirklich das gesichert, was Sie glauben, dass gesichert wird?

- Vorgängerversionen (Schattenkopien) - einschalten für die Datenpartition
- Backup der Datenpartition auf eine Sicherungspartition
- Backup des Datenverzeichnisses auf externe Datenträger (mittels Sicherungsskript) als Zuwachssicherung
- Aufbewahrung dieser externen Sicherungs-Datenträger
- Eine Backupgeneration außerhalb der Direktion (z. B. NAS im Serverraum), eine außer Haus aufbewahren – Sicherheit dieser Backups (verschlüsseln)!
- Diebstahl vom Direktionsgerät und/oder externer Sicherung

Daten bei Fremdanbietern

Haben Sie sich schon einmal überlegt, wo Sie überall Daten online speichern?

- Speichern Sie Ihre beruflichen bzw. schulischen Daten nur bei autorisierten Fremdanbietern online und damit außer Haus
  Lassen Sie sich in den jeweiligen Verträgen und Lizenzabkommen mit Ihnen bestätigen, dass sich diese Fremdanbieter von Softwarelösungen an die gesetzlichen Vorgaben, v. a. an das

  Datenschutzgesetz (DSG 2000) halten.
- Wir nehmen an, dass die Anbieter entsprechende Sicherungssysteme haben und kleineren und größeren technischen Pannen entsprechend vorbeugen, sodass es zu keinem Datenverlust kommen kann.
- Versuchen Sie trotzdem, Datenverlust bei Fremdanbietern durch lokale Sicherungen vorzubeugen und sichern Sie wichtige Daten (z. B. bei Anwendungen wie elektronisches Klassenbuch, Sokrates Web o.

Ä.) von Zeit zu Zeit auf Ihren lokalen Datenträgern. Es spricht nichts dagegen, in regelmäßigen Abständen beispielsweise Lehrstoffauswertungen, Zeugnisse, Stammblätter etc. als PDF lokal zu archivieren. Im Gegenteil: es gibt eine gewisse Sicherheit, dem Fall der Fälle ein wenig vorzubeugen.
- Bei Daten, die beim Dienstgeber oder Auftragsgeber liegen, können wir jedenfalls davon ausgehen, dass ein ausgeklügeltes Sicherheitskonzept zu Grunde liegt und Daten nicht "verloren gehen".

Aktuelle Software

Ist die installierte Software auf Ihrem Direktionsgerät am aktuellen Stand?

- Betriebssystem inkl. aktueller Service Packs (SP) und Updates
  (SP müssen teilweise manuell "angestoßen" werden
  --> MS/Windows Update suchen)
- Derzeit verwendbare MS Betriebssysteme:
  - MS Windows 10
  - MS Windows 8.1
  - MS Windows 7 mit SP 1
- Anwendungsprogramme inkl. aktueller Service Packs (SP) und Updates
  --> meist via Menüpunkt "Hilfe/?" – "Version/Info" bzw. "Auf Updates prüfen" zugänglich
- Derzeit verwendbare MS Office-Systeme:
  - MS Office 2016
  - MS Office 2013
- **Laufende/automatische Updates vom Betriebssystem und von den Anwendungsprogrammen**
- Verwenden legaler (lizensierter) Software
  (gecrackte Versionen beinhalten nebenbei erwähnt häufig Schädlingssoftware!)

Tipp 4:

MS Service-Pack-Center

Meine Windowsversion [1] (startet "winver.exe" in Ihrem Windows-Verzeichnis)

Firewall

Verwenden Sie die Windowsfirewall (Standard) oder eine alternative Firewall (evtl. von einer Antiviren-Internetsecurity-Lösung)?

- Aktiviert?
- Ohne Ausnahmen oder wenn - welche Ausnahmen sind eingetragen?

Antivirenprogramm

Die Verwendung eines gängigen, legalen, sprich gekauften und lizensierten Antivirenprogramms [2] wird dringend empfohlen!

- Inkl. Spam-, Spyware-, Adaware- und anderem Schädlingsschutz im Internet
- Aktuelle Virensigaturen
- Tägliche Updatesuche (in der Vormittagspause)
- Täglicher Schnellscan (in der Mittagspause)
- Wöchentlicher Deepscan
- ggf. als Task planen, falls nicht automatisch eingestellt

Sicheres Verhalten am Computer

Zum sicheren Verhalten am Computer gehören u. a. folgende Punkte:

- Aufstellort so wählen. dass Unberechtigte keinen Einblick haben
- keine Kennwort-Weitergabe
- Vertretung, Assistenz usw. müssen mit ihrem persönlichen Account, ansonsten mit einem Funktionsaccount für Anwendungen berechtigt werden
- Kennwörter regelmäßig ändern
- Bildschirmschoner mit Kennwort-Schutz bei Reaktivierung des Rechners
- "Never go without a screensaver!"
  Tastenkombination <WIN> + <L>
- bei längerer Abwesenheit (z. B. mehrere Stunden) Rechner ausschalten oder Ruhezustand
- Einschalten/Aufwecken nur via Powerknopf, Maus oder Tastatur,
  aber nicht via Netzwerkschnittstelle (--> "Wake-up-Ereignisse" im BIOS)
- nachhaltiges Löschen nicht mehr benötigter Datenträger
- Verdacht auf ein Sicherheitsproblem oder einen Sicherheitsvorfall unverzüglich Hotlinepersonen melden

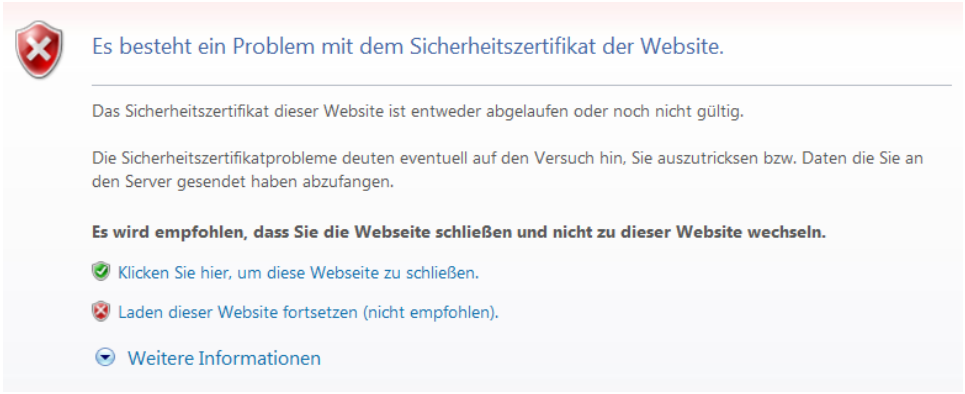
Tipp 5:

Wenn Sie den Verdacht haben, dass Ihr Kennwort einer dritten Person bekannt ist, ändern Sie es umgehend!

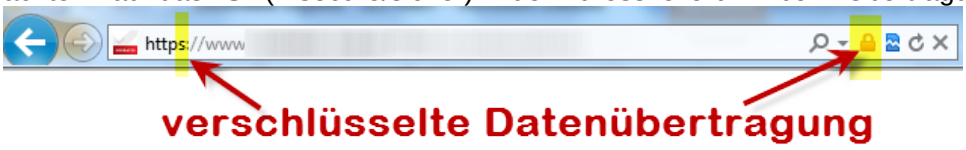
Sicheres Verhalten im Internet

Sicheres Verhalten im Netz besteht aus vielen Punkte - hier finden Sie eine kleine Auswahl:

- Zertifikatswarnungen beachten – nur fortsetzen, wenn Ihnen die Gefahr bewusst ist und wenn Sie wissen, was Sie tun!

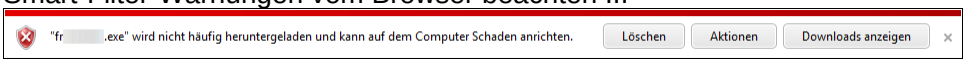


- Bei Anwendungen mit wichtigen/sensiblen Daten unbedingt auf den **verschlüsselten Datenverkehr** achten - auf das **"S"** (= secure/sicher) in der Adresszeile bzw. beim Übertragungsprotokoll ...

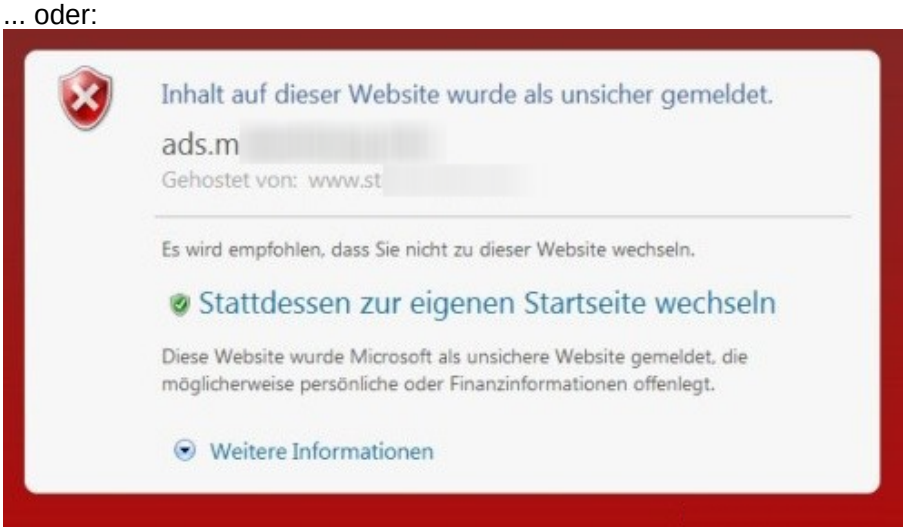


- ... sowie auf die Schlüssel- oder Zertifikatsinformationen!

- Auch beim E-Mail auf einen verschlüsselten Übertragungsweg Wert legen,
  imaps und pop3s (wenn pop3 schon sein muss)
  bzw. die Verschlüsselung beim Mailclient einschalten.
- Leseansicht beim Mailclient für die Ordner "Posteingang", "Junk-Mail" oder "Infected Mails" ausschalten.
- Keine Mails von unbekannten Personen mit zweifelhaftem Betreff öffnen,
  keine Anhänge solcher Mails öffnen,
  generell beim Öffnen von Mailanhängen mit ausführbaren Dateien (.exe, .com, .scr, …) sehr vorsichtig sein – nur solche ausführbaren Anhänge öffnen, die man von einer Gegenstelle erwartet oder angefragt hat.
- Smart-Filter-Warnungen vom Browser beachten ...



- ... oder:



Tipp 6:

Wenn Sie im Rahmen des Herunterladens zur unbeabsichtigten Installation von Software aufgefordert werden, brechen Sie den Vorgang sofort ab und verständigen Sie ggf. Ihre Hotline /Supportstelle!

Die folgenden 2 Punkte sind noch `in Ausarbeitung!`

Notebook - Netbook - Laptop

An welche sicherheitsrelevanten Probleme denken Sie im Zusammenhang mit den oben erwähnten Geräten?

Wenn Sie Informationen außerhalb Ihres Arbeitsplatzes, also unterwegs, zuhause etc. verwenden, legen Sie Wert darauf, diese Daten gut abzusichern!
Ein erstes Poblem ist Diebstahl, deshalb …

- Lassen Sie Ihre mobile devices nicht unbeaufsichtigt oder nicht sichtbar im Auto oder anderen Bereichen liegen.
- Speichern Sie keine vertraulichen oder sensiblen Daten lokal auf diesen Geräten - oder wenn,
- dann auf einer verschlüsselten Datenpartition bzw.
- externe Datenträger (wie externe Platten/USB-Sticks) - verschlüsselt - für die Datenspeicherung verwenden und getrennt aufbewahren/transportieren.
- Externe USB-Medien werden u. U. mit Verschlüsselungssoftware ausgeliefert
- USB Flash Security - praktikabel?
- Software zur Datenverschlüsselung ist z. B. "BitLocker" [3], "BitLocker to go" ist das freie Lesetool dazu;
- VeraCrypt praktikabel?
  Als Ersatz für "TrueCrypt" [4] samt Traveller-Modus
  oder "Free CompuSec"
- Wünschenswert wäre eine Software, die ohne merkliche Verzögerung "AES-256-Verschlüsselung" von den "Eigenen Dateien" (= Daten-Schule) in einem Container verschlüsselt bzw. die ganze Datenpartition ohne merkbare Geschwindigkeitseinbußen verschlüsselt und bei der Arbeit als Standardbenutzer verfügbar macht.

Das zweite Problem ist die unbeabsichtigte Datenfreigabe bzw. -preisgabe im Netz, wenn man via fremdes Netzwerk (Hotel, Flughafen, Seminarraum bei Fortbildungen, …) online geht - deshalb …

- ... alle Ordner- und Dateifreigaben abschalten!
- Versichern Sie sich, dass niemand Ihre vertraulichen Informationen mitliest - weder physisch noch technisch.

Smart Phones u. a. "intelligent devices"

Worin liegen die sicherheitsrelevanten Bedenken bei der Verwendung von sog. intelligenten Endgeräten wie SmartPhones?

Durch Synchronisierung sind häufig Kalender, Adressen, E-Mails, Dateien etc. lokal am mobilen Endgerät gespeichert. Und damit verbunden ist das erste Problem Diebstahl! Deshalb …

- ... Sperrung bzw. Rücksetzung vom SmartPhone via einschlägiger Internetanwendung ermöglichen
- ... Passwortsperre (PIN) jedenfalls einschalten
- plus (nach Möglichkeit) Mail-Passwort-Abfrage als Schutz des E-Mailverkehrs.

Das zweite Problem taucht evtl. auf, wenn man - s. o. - via fremdem Netz ins Internet geht.

Zu Hause arbeiten

Bei der Arbeit mit sensiblen Daten zu Hause gilt es folgende Überlegungen anzustellen:

- Wer hat Zugriff auf den Rechner?
- Mit welchem Konto und welchem Kontotyp (Berechtigung als Standardbenutzer oder Administrator)?
- Sind die schulischen Daten (Datenverzeichnis, Maildaten, …) vor dem Zugriff anderer User geschützt?
- Verwendung des Computers durch Kinder/Jugendliche, die mit oder ohne Freund/in evtl. unerwünschte oder unerlaubte Aktionen unternehmen und dabei Schädlingssoftware auf den Rechner bringen?

Abschließende Überlegungen

Siehe dazu Security theoretisch.

1
Alternativ klicken Sie: <Start>-<Ausführen> und geben den Befehl "c:\windows\system32\winver.exe" ein.

2
Grundsätzlich gibt es im schulischen Umfeld kein Gratis-Antivirenprogramm - abgesehen von 30-/60-/90-Tage-Testversionen. Es sei denn, Sie haben von einem Hersteller eine besondere Lizenz erhalten, die den kostenlosen Einsatz in der Schule erlauben würde. Die uns bekannten sog. freien Antivirenprogramme sind meist nur für den privaten Gebrauch ("home-use") lizenzrechtlich einsetzbar und in den allermeisten Fällen ist der Einsatz im schulischen Umfeld, im Verwaltungsbereich oder im akademischen Bereich nach dem Lizenzrecht des Herstellers nicht erlaubt. Die meisten Hersteller bieten aber Schullizenzen an, die preislich stark reduziert sind.

3
Die Festplattenverschlüsselungs-Software BitLocker von der Fa. Microsoft ist bspw. ab dem Betriebssystem Windows 7 in der Ausführung Enterprise und ab Windows 8.1 Pro enthalten.

4
Das kostenlose Open-Source-Programm

VeraCrypt

eignet sich zum sicheren Verschlüsseln einzelner Daten, einzelner Verzeichnisse, externer Speichermedien oder von Partitionen bis hin zum kompletten System.